~~CONFIDENTIAL//SI//REL TO USA, FVEY~~

SIGNALS INTELLIGENCE DIRECTORATE

MANAGEMENT DIRECTIVE 427

Issue Date: 01 August 2009
Revised Date: 28 December 2013
Second Rev: 14 September 2015

POC: S02

(U) ACCESS TO CLASSIFIED U.S. INTELLIGENCE INFORMATION FOR SECOND PARTY PERSONNEL

(U) Purpose

(U//~~FOUO~~) This document provides guidance for granting Second Party SIGINT personnel access to classified U.S. intelligence information in accordance with Department of Defense Directive (DoDD) C-5230.23, "Intelligence Disclosure Policy" (Ref A); Director of Central Intelligence Directive 6/7, "Intelligence Disclosure Policy" (Ref B); and DoDD 5240.1-R, "Procedures of DoD Intelligence Components that Affect U.S. Persons" (Ref C)

NOTE: *(U) Underlined terms are defined under Annex D Definitions.*

(U) Scope

(U) This Signals Intelligence Directorate (SID) Management Directive applies to all U.S. SIGINT production elements located at NSA Headquarters (NSAW) and across the United States SIGINT System (USSS).

(U) This guidance supersedes all previously approved SIGINT Directorate guidance and authorizations for Second Party access to classified U.S. intelligence information. Second Party personnel who require access for the performance of the SIGINT mission must be re-justified and resubmitted for approval by the SIGINT Director or Deputy Director.

(U) All new requests for Second Party accesses after the date of issue of this document must follow the guidelines herein.

//s//

RONALD S. MOULTRIE
Signals Intelligence Director

DISTRIBUTION:
Signals Intelligence Directorate, All
SIGINT Enterprise, Field, All
Office of General Counsel
Office of Corporate Policy

(U) BACKGROUND

(U) Background

1. (U) NSA/CSS has a tradition of signals intelligence (SIGINT) collaboration with its Second Party SIGINT Partners that has served us well. NSA/CSS and the Intelligence Community (IC) have benefited from this exchange and have broadened and improved U.S. knowledge and capabilities. Notwithstanding our special partnerships with our Second Party SIGINT Partners, NSA/CSS must first ensure that activities with our partners comply with all U.S. legal and policy guidelines. This management directive is established to define, document, and implement internal procedures to ensure consistency and compliance with all legal and policy guidelines.

2. (U) Granting access to Second Party personnel to classified U.S. intelligence information must be done in accordance with procedures established within NSA/CSS and consistent with policies and procedures of the Director of National Intelligence and the Secretary of Defense. In addition, NSA/CSS, first and foremost, has a responsibility to protect intelligence information that contains or may contain equities of other members of the IC. Granting access to or approving release of information to Second Party personnel applies equally to SIGINT as well as to intelligence gathered under the authority of other IC agencies, or any intelligence from those agencies that is fused with SIGINT (to include that from collaborative access efforts). Often, only the originating agency or element may be aware of the sensitivities of the intelligence information, therefore that agency's permission must be obtained prior to sharing.

3. (U//~~FOUO~~) Per Director of Central Intelligence Directive (DCID) 5/5P, "Conduct of Liaison with Foreign Governments and Release of U.S. SIGINT to Foreign Governments" (Ref D), DIRNSA/CHCSS is the executive agent of the U.S. Government for the conduct of SIGINT arrangements with the Second Parties. DCID 6/6, "Security Controls on the Dissemination of Intelligence Information" (Ref E), specifies that intelligence may be shared with foreigners (including Second Party personnel) to the extent such sharing promotes the interests of the United States, is consistent with U.S. law, does not pose unreasonable risk to U.S. foreign policy or national defense, and is limited to a specific purpose and normally of limited duration. The directive mandates NSA/CSS' responsibility to apply appropriate controls to and accountability for the access to or release of intelligence to our foreign partners.

(U) Data Categories

4. (U//~~FOUO~~) For the purposes of this policy, data, databases, and data sets maintained by NSA/CSS will be categorized as follows:

(b)(3)-P.L. 86-36

(U) POLICY

(U) Approval Authorities

5. (U//~~FOUO~~)

6. (U//~~FOUO~~)

7. (U//~~FOUO~~) If the Second Party person is an integree as defined in NSA/CSS Policy 1-13, "Second Party Integrees" (Ref F), then will be recorded by the integree's supervisor and the appropriate Foreign Affairs Directorate desk officer shall be notified.

8. (U//~~FOUO~~) Second Party personnel access to NSA/CSS-maintained databases or data sets that only contain classified information marked releasable to that partner or databases that are capable of restricting access only to that data which is marked releasable to that partner, regardless of the originating agency of the data, will be granted to Second Party personnel in accordance with Annex A to this policy. Approval authority for Second Party access marked releasable resides with the relevant SIGINT Directorate Deputy Director or Associate Director (i.e., DDEM/ADDEM, DDAP/ADDAP, DDDA/ADDDA, and ADD/SSG), NTOC DIR, and SUSLOs Canberra, London, Ottawa, and Wellington).

(b)(3)-P.L. 86-36

9. (U//~~FOUO~~)

(U//~~FOUO~~)

[redacted]

~~NOTE: (U//FOUO)~~ [redacted]

(b)(3)-P.L. 86-36 [redacted]

10. (U//~~FOUO~~) [redacted]

[redacted]

11. (U//~~FOUO~~) The NSA/CSS Director, the NSA/CSS Deputy Director, or authorized Designated Intelligence Disclosure Officers (DIDOs) may authorize release to a Second Party Integree of classified U.S. intelligence that bears no specific control markings (i.e., that is not marked with "NOFORN," "REL TO," or another control marking such as "ORCON"). The details of the DIDO program and authorities may be found in DCID 6/7, "Intelligence Disclosure Policy," and the list of designated NSA/CSS DIDOs.

(U) Data Uses

12. (U//~~FOUO~~) Access to data by or release of data to Second Party personnel does not convey authorization or approval for Second Party follow-on use. Further use guidance will accompany each Second Party access provision.

(b)(3)-P.L. 86-36 [redacted]

(U) Termination of Access	15. (U//~~FOUO~~) When a Second Party person changes work assignments or locations, any access to NSA/CSS maintained data, databases, or data sets granted through an NSA/CSS approval process (such as the SIGINT Contact Center (SCC)) is similarly terminated in accordance with SID Management Directive 421, "United States SIGINT System Database Access" (Ref H).
(U) Emergencies	16. (U) For emergency sharing authorization, the NSA Director or Deputy Director and/or the SIGINT Director and Deputy Director are the sole approving authorities. Emergency situations are defined and will be implemented per guidance in DCID 6/6, Section 10.

(U) ANNEX A
ACCESS TO RELEASABLE DATA

(U) General	A.1. (U//~~FOUO~~) Second Party personnel, whether integrated into an NSA/CSS established SIGINT production element or assigned to a Second Party SIGINT organization, may be granted access to NSA/CSS maintained SIGINT databases and data sets that contain only data marked as releasable to that Second Party partner or databases that are capable of restricting access only to that data which is marked as releasable to that partner. All Second Party personnel accessing NSA/CSS maintained databases and data sets must adhere to the same standards as U.S. SIGINT personnel with regard to U.S. intelligence oversight, to include U.S. Intelligence Oversight Officers (IOOs), U.S. auditors, and appropriate intelligence oversight training and reporting programs. Second Party Integrees shall not be assigned positions for which access to NOFORN information is routinely required, without prior approval from all originators of that information.
(U) Access for Personnel in Second Party SIGINT	A.2. (U//~~FOUO~~) Second Party SIGINT elements requiring access to releasable databases or data sets must first be registered in the NSA/CSS Mission Correlation Table (MCT) in accordance with SID Management Directive 422, "USSS Mission Delegation" (Ref I), by following the SID SIGINT Contact

Elements

Center (SCC) process [redacted] for Sponsors and Data Masks. Given that these will be Second Party missions, the relevant Analysis and Production Global Capability Managers will coordinate on, but not approve, the registration of the mission and the associated databases.

(b)(3)-P.L. 86-36

A.3. (U//~~FOUO~~) Second Party SIGINT elements will work with the appropriate Senior U.S. Liaison Office (SUSLO) and the appropriate NSA/CSS Foreign Affairs Directorate (FAD) Desk Officer to draft and coordinate the access request for registration in the MCT. The FAD Desk Officer will function as the Sponsor into the SCC process. The Desk Officers will work with SID Oversight and Compliance (O&C) Compliance and Verification Team [redacted] to determine the appropriate oversight path, training, and auditing requirements for each element and associated database being registered in the MCT. If access is approved, access to individual releasable databases is then granted through the SCC standard procedure.

(U) Access for Second Party Integrees

A.4. (U//~~FOUO~~) Second Party SIGINT personnel integrated into NSA/CSS SIGINT production elements under NSA/CSS Policy 1-13, "Second Party Integrees" will be sponsored for access through established procedures in SIGINT Management Directive 421. Supervisors of Second Party integrees must maintain a list of any databases or data sets accessed by the integree and will notify the appropriate FAD Desk Officer of any changes during the integree's assignment which would require a change to access. Approval authority for database and/or data set access to "NSA/CSS or IC Not-Releasable" will be the NSA Director, Deputy Director, SIGINT Director or SIGINT Deputy Director.

(U) Termination of Access

A.5. (U//~~FOUO~~) When Second Party personnel change work assignments or locations, any access to SIGINT databases or data sets will be terminated immediately. The SIGINT production element's NSA/CSS Sponsor or Intelligence Oversight Officer (IOO) is responsible for requesting the database System Administrators to terminate and remove the individual's accounts from their systems in accordance with SID Management Directive 421. For Second Party Integrees, the immediate supervisor (U.S. or Second Party) is responsible for the termination of accesses and will notify the appropriate FAD desk officer and personnel in accordance with SID Management Directive 421.

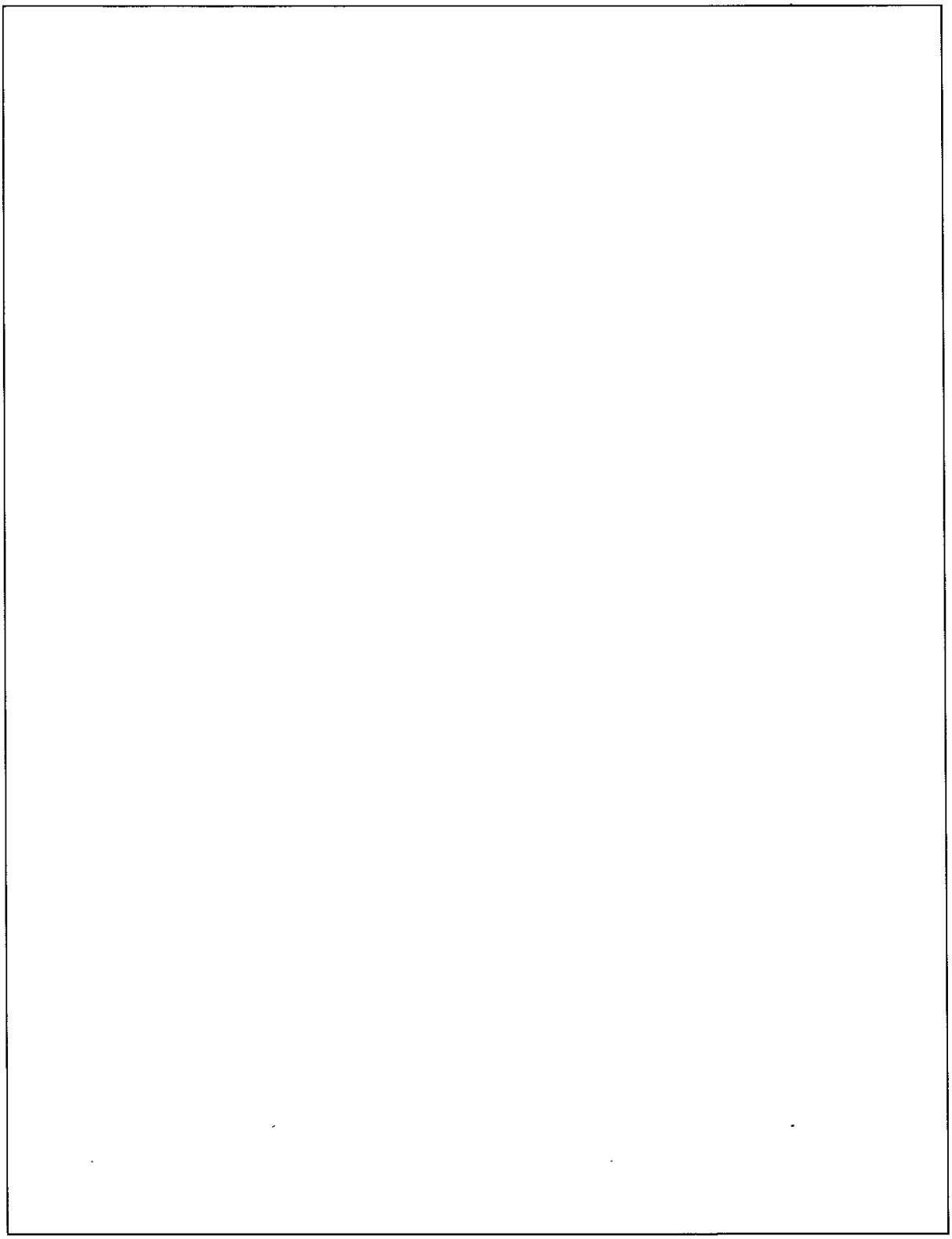
(b)(3)-P.L. 86-36

(U) ANNEX B

[redacted]

(b)(3)-P.L. 86-36

~~CONFIDENTIAL//SI//REL TO USA, FVEY~~



(b) (3)-P.L. 86-36

(U) ANNEX C
REFERENCES

a. (U//~~FOUO~~) Department of Defense Directive (DoDD) C-5230.23, "Intelligence Disclosure Policy"

b. (U//~~FOUO~~) Director of Central Intelligence Directive 6/7, "Intelligence Disclosure Policy"

c. (U//~~FOUO~~) DoDD 5240.1-R, "Procedures of DoD Intelligence Components that Affect U.S. Persons"

d. (U//~~FOUO~~) Director of Central Intelligence Directive (DCID) 5/5P, "Conduct of Liaison with Foreign Governments and Release of U.S. SIGINT to Foreign Governments"

e. (U//~~FOUO~~) Director of Central Intelligence Directive (DCID) 6/6, "Security Controls on the Dissemination of Intelligence Information"

f. (U//~~FOUO~~) NSA/CSS Policy 1-13, "Second Party Integrees"

g. (U//~~FOUO~~) NSA/CSS POLICY 1-41, "The NSA/CSS Exceptionally Controlled Information (ECI) System"

h. (U//~~FOUO~~) SID Management Directive 421, "United States SIGINT System Database Access"

i. (U//~~FOUO~~) SID Management Directive 422, "USSS Mission Delegation"

j. (U//~~FOUO~~) Executive Order (E.O.) 12333, "United States Intelligence Activities"

k. (U//~~FOUO~~) National Security Act of 1947

l. (U//~~FOUO~~) UKUSA Agreement, dated 5 March 1946

(U) ANNEX D
DEFINITIONS

(U) Data Set

D.1. (U) For the purpose of this policy, a large collection of intelligence data that has not been evaluated for foreign intelligence or minimized to protect U.S. identities but is not a formal database subject to the SIGINT Contact Center (SCC) process or a similar access control. A data set may also be a data feed such as would be needed for a research/development effort.

(U) Database

(b)(3)-P.L. 86-36

D.2. (U//~~FOUO~~) For the purpose of this policy, a structured collection of records or data that is stored in a computer system and organized in a data management system for quick retrieval of those records. A database is generally subject to the SCC process or a similar access control and listed

(U) Designated Intelligence Disclosure Official (DIDO)

D.3. (U) The heads of departments and agencies with organizations in the Intelligence Community or the heads of such organizations, and their specifically designated subordinates whose names and positions are certified to the Director National Intelligence (DNI) in writing, and other U.S. officials designated by the DNI.

(U) Exceptionally Controlled Information (ECI)

D.4. (U) COMINT sub-control system/sub-compartment to protect TOP SECRET exceptionally sensitive COMINT sources, methods and activities.

(U) Evaluated, Minimized Traffic (EMT)

D.5. (U) Traffic that has been minimized for U.S. identities and assessed for foreign intelligence value.

(U) Integree

D.6. (U//~~FOUO~~) The term "integree" in this document refers to Second Party Partner personnel integrated into or detailed to SIGINT production element (as defined in USSID CR1610) who, when integrated into an NSA/CSS environment, are working solely under the direction and operational control of the DIRNSA/CHCSS to conduct SIGINT activities that support information needs validated by NSA/CSS in accordance with NSA/CSS authorities, rules, and regulations. Integrees may be civilians or military members. Integrees must be approved in accordance with NSA/CSS Policy 1-13, "Second Party Integrees."

(U) Intelligence

D.7. (U) Includes the following information, whether written or in any other medium, classified pursuant to Executive Order 12958 or any predecessor or successor Executive Order:

a. (U) Foreign intelligence and counterintelligence defined in the National Security Act of 1947 (Ref K), as amended and Executive Order 12333;
b. (U//~~FOUO~~) Information describing U.S. foreign intelligence and counterintelligence activities, sources, methods, equipment, or methodology used for the acquisition, processing, or exploitation of such intelligence; foreign military hardware obtained through intelligence activities for exploitation and the results of the exploitation; and any other data resulting from U.S. intelligence collection efforts; and

(U) Information on Intelligence Community protective security programs (e.g. personnel, physical, technical, and information security).

(U) Intelligence Community (IC)

D.8. (U) The Intelligence Community comprises the:

- Central Intelligence Agency (CIA),
- National Security Agency (NSA),
- Defense Intelligence Agency (DIA),
- Bureau of Intelligence and Research (within the Department of State),
- National Geospatial-Intelligence Agency (NGA),
- National Reconnaissance Office (NRO),
- Intelligence and Counterintelligence Elements of the Army, Navy, Air Force, Marine Corps, and Coast Guard.
- Staff elements of the Director of National Intelligence (DNI), and
- Intelligence elements of the:

- Drug Enforcement Administration,
- Federal Bureau of Investigation (FBI),
- Department of Justice,
- Department of the Treasury,
- Department of Homeland Security, and
- Department of Energy.

(U) SIGINT Content

D.9. (U) The actual information (e.g., voice, data, or video) exchanged between one or more individuals, systems or devices.

(U) SIGINT Metadata

D.10. (U//~~FOUO~~) Refers to structured "data about data." Metadata includes all information associated with, but not including content, and includes any data used by a network, service, or application to facilitate routing or handling of a communication or to render content in the intended format. Metadata includes, but is not limited to, dialing, routing, addressing, or signaling information and data in support of various network management activities (e.g. billing, authentication or tracking of communicants).

(U) Mission Correlation Table (MCT)

D.11. (U//~~FOUO~~)

(b)(3)-P.L. 86-36

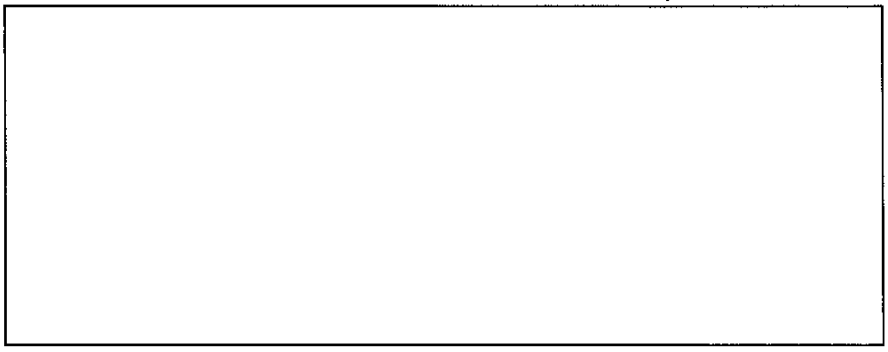
(U) Product

D.12. (U) Foreign intelligence (derived from SIGINT processes) that is made available in readable form to authorized recipients in response to stated or implied Information Needs. SIGINT Product reporting standards are governed United States Signals Intelligence Directives (USSIDs) and other SIGINT policy.

(U) Raw SIGINT Data

D.13. ~~(C//SI//REL TO USA, FVEY)~~ Raw SIGINT data is any SIGINT data acquired either as a result of search and development or targeted collection operations against a particular foreign intelligence target **before** the information has been evaluated for foreign intelligence AND minimization purposes. It includes, but is not limited to, unevaluated and/or unminimized

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36



(U) Second Party

D.14. (U) Any of the four countries with which the U.S. Government maintains close, cooperative SIGINT and Information Assurance (IA) relationships: Australia, Canada, New Zealand, and the United Kingdom (UK). The strategic alliance among these nations stems from the strong cryptologic partnerships that developed during World War II and were first formalized in the UKUSA Agreement (Ref L), dated 5 March 1946.

(U) Second Party SIGINT Partners

D.15. (U) The following SIGINT organizations, their subordinate units, and other cryptologic units affiliated with, or approved by, the National SIGINT authority. The organizations are:

a. (U) UK - Government Communications Headquarters (GCHQ)

b. (U) Canada - Communications Security Establishment Canada(CSEC)

c. (U) Australia - Defence Signals Directorate (DSD)

d. (U) New Zealand - Government Communications Security Bureau (GCSB)

(U) Second Party SIGINT Personnel

D.16. (U) This includes all Second Party personnel assigned to and working under the SIGINT Authorities of the respective Second Party Partner organization. This includes Second Party civilian, military, and contractor personnel.

(U) SIGINT Production Element

D.17. (U) A formally recognized and documented element (organization, unit) that executes at least one of the SIGINT production functions (collection, processing, analysis, retention, and dissemination) performed by United States SIGINT System (USSS) and/or foreign SIGINT production personnel (collectors, cryptanalysts, intelligence analysts, linguist, reporters, SIGINT development analysts, research personnel, staff, support elements, and managers) necessary for the conduct of an assigned SIGINT mission.

(U) Stakeholder

D.18. (U) Stakeholders in the access of data Not Releasable by a Second Party person would be any office with an equity in the information. This list might include:

- S1 Customer Relations,
- S2 Analysis and Production,
- S3 Data Acquisition,
- SSG SIGINT Development,
- Associate Deputy Directorates for Counter Terrorism (ADD/CT) and Technical SIGINT and Electronic Warfare(ADD/TSE),
- National Threat Operations Center (NTOC),
- NSA/CSS Commercial Solutions Center (NCSC),
- Research Directorate (RAD),
- Associate Directorate for Education and Training (ADET),
- Associate Directorate for Security and Counterintelligence (ADS&CI), and
- National Cryptologic Representatives and Senior Liaison Officers, as appropriate.

(U) United States SIGINT System (USSS)

D.19. (U) The United States SIGINT System (USSS) is the SIGINT part of the United States Cryptologic System (USCS) and refers to the U.S. Government SIGINT activities worldwide under the direction of the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS). The USSS is composed of the NSA/CSS SIGINT Directorate, the SIGINT functions and elements of the military departments, and other governmental elements (other than the Federal Bureau of Investigation) authorized to perform SIGINT activities under the direction and authority of the DIRNSA/CHCSS.